



Department of Veterans Affairs Office of Information and Technology

VA IT Governance Plan

March 12, 2007

Version 8.3

Contents

Executive Summary	1
1 Introduction	3
2 IT Governance Overview.....	6
2.1 The Need for IT Governance	6
2.2 IT Governance Focus Areas	6
2.2.1 Strategic Alignment.....	7
2.2.2 Value Delivery (Value Creation)	8
2.2.3 Risk Management (Value Assurance)	8
2.2.4 Resource Management.....	9
2.2.5 Performance Measurement	9
2.2.6 Linking the Five Focus Areas of IT Governance to the VA.....	10
2.3 VA-Wide Governance and VA IT Governance	11
2.3.1 VA-Wide Governance	11
2.3.2 VA IT Governance	12
3 VA IT Governance Model	13
3.1 IT Governance Guiding Principles	13
3.2 IT Governance Decisions.....	14
3.3 VA IT Governance Boards	15
3.3.1 Strategic Management Council (SMC)	19
3.3.2 IT Leadership Board (ITLB)	19
3.3.3 Business Needs and Investment (BNI) Board	19
3.3.4 Planning, Architecture, Technology and Services (PATs) Board	20
3.3.5 Business Advisory Committee	20
3.3.6 Other IT Governance Bodies	21
3.3.7 Example IT Governance Decision	21
3.3.8 Board Charters.....	23
3.4 Road Map for Implementing IT Governance	23
3.5 VA IT Governance Summary	24
Appendix A. Reference.....	26
Appendix B. IT Governance Framework.....	27

Figures

Figure 1 - IT Governance Focus Areas.....	10
Figure 2 - Where IT Governance Fits into Governance at the VA.....	11
Figure 3 - IT Governance Guiding Principles for the VA.....	13
Figure 4 - Systems Development Life Cycle (SDLC).....	16
Figure 5 - VA IT Governance Board Structure.....	17
Figure 6 - Example IT Governance Decision Flow Chart	22
Figure 7 - Road Map for IT Governance Implementation	23
Figure 8 - IT Governance Schools of Thought Drawn On	28

Table

Table 1 - VA IT Governance Boards..... 18

Executive Summary

The VA IT Governance Plan describes, how IT Governance relates to governance at the Department of Veterans Affairs (VA), and the planned approach to enhancing the VA's IT Governance. The goals of this document are to explain the criticality for more effective IT Governance, what more effective IT Governance entails, and to describe the VA IT Governance Model. Implementing this model will enable the VA to better align IT strategy to business strategy, maintain and develop the Enterprise Architecture, enhance Information Protection/Data Security, manage the IT investments, and reconcile disputes regarding IT.

IT Governance is the vehicle that enables the OI&T to centralize its IT decision making. The link between IT Governance and OI&T is crucial, because IT Governance will ensure the alignment of IT strategy, systems and processes to the VA's business strategy. This alignment creates benefits for veterans, service members, employees, other beneficiaries, and stakeholders. These benefits include cost savings, increased efficiency and efficacy, information security (through the "Gold Standard" for data security), faster and easier access to information, improved service and greater reliability.

For the OI&T to operate effectively, all five focus areas of IT Governance must be addressed (see Figure 1, pg. 9) including: strategic alignment, value delivery, risk management, resource management, and performance management.

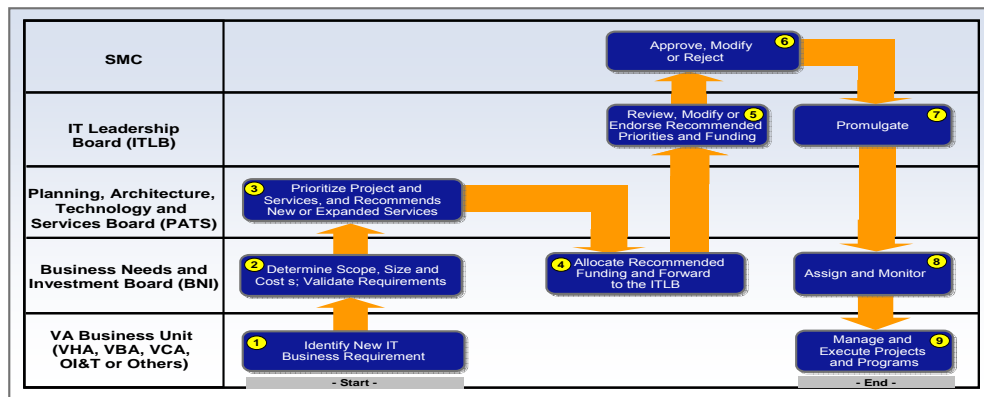
- "Strategic Alignment" is aligning the IT strategy to the VA-wide business strategy and assessing the VA-wide IT needs.
- "Value Delivery" implies that the VA needs to raise the Capability Maturity Model (CMM) rating across all of the Departments so that IT is part of an integrated Department-wide capability to enable new processes in the Administrations and Staff Offices to provide better healthcare, benefits, and other services to its customers.
- "Risk Management" requires focus on reducing the IT risks to the VA and to protect its employees', our veterans' and their dependents' information and the VA infrastructure.
- "Resource Management" provides guidance to the VA for providing quality human and non-human resources to increase the effectiveness of employee hiring and retention, and it improves procurement.
- "Performance Measurement" relates to the VA's ability to measure and manage its budget, serve our employees', veterans' and their dependents' needs, train its employees, and generally operate effectively and efficiently.

At the VA, IT Governance is the responsibility of the VA Executive Board, the Strategic Management Council (SMC) and other executive managers; it is not just the responsibility of the OI&T. IT Governance is an integral part of Department-wide governance and aligns to the VA's business strategies and objectives. Trust must be built among the stakeholders in the management of information and technology in the Department. Implementing VA IT Governance involves shared decision making through the IT Governance boards, based on the guiding principle of aligning IT strategy and goals to business strategy and goals.

IT Governance Guiding Principles: The establishment of IT Governance Guiding Principles is a critical success factor for the implementation of a single authority IT leadership model. The guiding principles must specify the input rights, decision making authority and accountability to direct correct behavior in the use of IT. The VA IT Governance Guiding Principles emphasize: Administrations and Staff Offices determine business requirements, projects and priorities; OI&T determines the IT solutions and manages the IT portfolio; the VA CIO is the manager of IT resources and IT program execution; IT Governance policy must be explicit and communicated; and that IT Governance is part of and aligns with Department-wide governance.

IT Governance Decisions: The three types of IT Governance decisions are Enterprise Architecture, IT Stakeholder (Administrations and Staff Offices) Requirements, and IT Investments. Enterprise Architecture must meet legal standards, be agreed upon by VA leadership, align with the VA-wide strategic plan, and create IT infrastructure that is a best fit for current and emerging VA IT needs. IT Stakeholder Requirements determine the functional requirements. IT Investments determine the degree of strategic alignment, the programming and budgeting of resources against the IT business plan, and its ability to meet customer demand, the priorities, and the funding allocation according to the Administrations' and Staff Offices' needs and requirements. The IT Governance Boards are not involved in day-to-day IT Governance decision making. Instead the boards are responsible for VA-wide IT strategy, policy, program and investment setting decisions; and serve to resolve issues that have been escalated after failure in resolution at lower decision making levels in OI&T or other VA Administrations and Staff Offices.

IT Governance Governing Boards: The four IT Governance Boards are the *Strategic Management Council (SMC)*, the *IT Leadership Board (ITLB)*, the *Business Needs and Investment (BNI) Board*, and the *Planning, Architecture, Technology and Services (PATS) Board*. The SMC serves as the senior board making decisions related to IT strategy and technology, decides the overall level of IT spending, aligns and approves Enterprise Architecture, accepts IT risks, provides final approval, and resolves disputes of the ITLB. The ITLB aligns IT goals with business goals, determines achievement of IT goals, develops and approves the IT budget and programs, and resolves issues for BNI and PATS. The BNI confirms business needs and requirements, oversees risk, reviews funding costs and investments, formulates and approves IT budgets and programs, and monitors IT budget execution. The PATS designs, tailors and updates as needed the IT Enterprise Architecture; recommends IT direction, resolutions and new services; develops information security architecture; evaluates business project priorities; and makes Department-wide IT recommendations. Below is an example of how an IT Governance decision may flow among the boards.



Note: Snapshot of “Figure 6 – Example IT Governance Decision Flow Chart”
(for more information see Figure 6, pg. 21)

Road Map for IT Governance Implementation: Based on industry-wide best practices there are five stages for implementing IT Governance: (1) Identify Needs, (2) Envision Solution, (3) Plan Solution, (4) Implement Solution and (5) Operationalize Solution. At the VA much of the initial work has already begun and is in various stages of completion. The road map is a tool for ensuring all aspects of IT Governance are both recognized and tailored to meet the VA’s current and emerging IT needs. The road map should be implemented immediately.

Summary: The IT Governance boards must be operated and managed by well qualified and knowledgeable individuals who understand VA’s various business and IT strategies, processes, programs and goals. Transparency in deliberating and decision making are needed so that trust and regard for the VA’s high priority needs and risks are addressed judiciously, thoroughly, and in a way that supports One-VA. IT Governance will yield improvements in the areas of: standardized processes, alignment of IT to business strategy, realization of business goals, cost effectiveness, and better service to veterans, service members, employees, and other beneficiaries and stakeholders.

1 Introduction

The Department of Veterans Affairs (VA) is transforming its Office of Information and Technology (OI&T) into a centralized IT Management System model. Inherent to this process is the need to build the *relationships* and *processes* to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. *IT Governance Imperatives* that build the foundation for this successful transition are "Building Trust" and Building Partnerships".

IT GOVERNANCE IMPERATIVES

BUILD TRUST

- Trust must be built among the stakeholders in the management of information and technology in the Department
- Trust is not achieved in documents; it is achieved through cooperative partnerships between the business needs of the Administrations and Staff Offices and the IT service provider – OI&T
- Structure along without a foundation of trust can't function
- IT Governance provides the requisite foundation to address the central theme of concern – how to establish trust among stakeholders in the management of information and technology in VA

BUILD PARTNERSHIPS

- IT Governance is not an isolated discipline.
- IT Governance should form an integral part of VA Governance and needs to be addressed at the most senior levels of leadership.
- IT Governance is structure of relationships and processes to direct and control the VA to achieve its Department-wide goals by adding value, while balancing risk versus return over IT and its processes.
- Senior leaders must ensure that IT operational risks are mitigated and the value that is returned by technology investments meet the strategic goals and objectives of the VA.
- Day-to-day communication between the Administrations and Staff Offices with various OI&T offices will continue and is encouraged in order to ensure close coordination between the businesses and OI&T.

The scope of this document is to define IT Governance and its application within the Department of Veterans Affairs. The purpose of this document is to define and describe: IT Governance, the VA IT Governance Guiding Principles, the VA IT Governance Model, and the Road Map for Implementing VA IT Governance.

To provide a context for IT Governance at the VA, the VA IT strategy for FY 2006-2011 is described in this section. Objective E3 of the VA Strategic Plan FY 2006-2011 is to: ***"Implement a One-VA information technology (IT) framework that enables the consolidation of IT solutions and the creation of cross-cutting common services to support the integration of information across business lines and provide secure, consistent, reliable, and accurate information to all interested parties."***

VA's IT transformation aligns to Objective E3 through three main goals:

- 1- Achieve a Gold Standard for IT Security
- 2- Maintain IT Systems to continue providing current IT services to veterans, service members, employees, other beneficiaries, and stakeholders.
- 3- Enhance and develop IT services to veterans, service members, employees, other beneficiaries, and stakeholders.

Achieving the VA IT transformation goals requires implementing an Enterprise Architecture (EA) program that is business-driven and provides information, products, and services that enable the VA IT community to develop and maintain business-focused, veteran-centric, and enterprise-wide IT systems, data, and infrastructure. As identified by the VA Chief Information Officer (CIO) four principles form the cornerstone for how IT systems and infrastructure will support the VA:

- Veteran access to VA services must be available via the Web and/or other technology channels, and must facilitate self service;
- Customer-focused, service oriented systems, applications, and data must be shared and accessible to all possible users;
- VA's infrastructure must be self-healing, robust, and always transparent; and
- VA's data must employ a storage-centric strategy that supports enterprise storage methods, in order to facilitate efficient use and sharing of data by business stakeholders and applications across the Department.

During the FY 2006-2011 timeframe, the implementation of several IT-centric strategies and initiatives will ensure that VA's IT systems, data, and infrastructure will support the business of the VA most effectively in serving the veterans, service members, employees, other beneficiaries, and stakeholders. These strategies and initiatives include: Application and Consolidated Shared Services; the realigned IT management system; ensuring information security through the evolving Gold Standard for Data Security; establishing an Enterprise Privacy Program (EPP); continuing to evolve the Enterprise Project; establishing a One-VA telecommunications network; advancing the VA's medical records; maintaining Corporate Data Warehouse; enhancing the Veteran Health Information Systems and Technology Architecture (VistA); building and expanding the use of the Veteran's information portal and My HealthVet to increase benefit delivery and self service; expand HealthVet -2012; improving and expanding Home-Telehealth; improving collaboration with DoD; and expanding E-Government.

These IT centric strategies and initiatives will hold great value and benefit for the VA businesses and customers both internally (Administrations, Staff Offices, managers and employees) and externally (veterans, service members, other beneficiaries, and stakeholders). Data sharing, storage and security will be advanced. Greater electronic access will be made available to patient records and other customer data; so, service will be more reliable, faster and more secure. Communications will be more integrated, faster, and more reliable. Collaboration with external business partners to the VA, such as the DoD, will be enhanced. In general, the increased efficiency and effectiveness of the VA IT infrastructure that will occur as a result of the FY 2006-2011 strategies and initiatives will save money, provide better existing services, and provide the infrastructure capacity to add new services based on the emerging needs of VA customers.

In 2006, security was pinpointed as an area that must be improved to better protect the personal information of the VA's customers internally and externally. Realizing the need for improved data security, OI&T has made achieving the "Gold Standard" for Data Security an essential component to achieving the VA IT strategies and initiatives successfully. Information Security Governance is enabled by Information Security Policy. Information Security is an essential component of IT Governance. The VA Information Security Policy will address the fundamentals of agency Information Security structure including: information security roles and responsibilities; a statement of the security control baseline and rules for exceeding the baseline; and rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance. The Gold Standard for Data Security also relies on IT strategic planning, training and education, security measures and monitoring, securing of devices, encryption of data, enhanced data security for VA's sensitive information, enhanced protection for shared data in interconnected systems, and incident management and monitoring.

A critical aspect of the VA IT Governance Plan is to assure it maintains a *Federal Alignment* with all aspects of Federal Policies, Acts, and Circulars regarding Federal IT governance and management. As part of the continuing enhancements of this IT Governance Plan, the development of the various charters and guidelines will serve as the mechanism to ensure compliance with Federal mandates.

It is clearly understood that the IT Governance Plan will ensure and address within its charters and operating procedures the following requirements: (a) the Federal Managers' Financial Integrity Act (FMFIA); (b) the Federal Information Security Management Act of 2002 (FISMA); (c) the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act); (d) the Privacy Act and the Health Insurance Portability and Accountability Act; (e) Office of Management and Budget Circular A-127, *Financial Management System*; and (f) the E-Government Act of 2002.

Furthermore we will glean our guidance from OMB Circular #A-123, which provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations. In addition, the Federal Information Security Management Act of 2002, which requires a combination of Federal information processing standards and the special publications SP-800 series issued by the National Institute of Standards and Technology, will be followed and included into the respective areas as applicable within charters and guidelines of the governing bodies.

IT governing bodies will include in their charters the requirement to resolve issues to ensure that the improvement of efficiency and effectiveness of the Department's IT operations and the delivery of IT services. This will be achieved by capturing, monitoring and making sound decisions that (1) address performance measurements prescribed for information technology; (2) quantify benchmarks in terms of cost, speed, productivity, and quality of outputs and outcomes; and (3) ensure compliance with information security policies, procedures, and practices. Additionally, this IT Governance Plan is not intended to and will not contradict the statutory authority and functions of the VA's Chief Financial Officer (CFO).

This document is organized into three sections and two appendices.

Section 1: Introduction: defines the document purpose and objectives.

Section 2: IT Governance Overview: describes what IT Governance is and what it offers to the VA IT Realignment Program.

Section 3: VA IT Governance Model: provides a description of IT Governing Principles, IT Governance Decisions, VA IT Governance Boards, and the VA IT Governance Approach.

Appendix A. Reference, describes parent and reference documents on which this document was based.

Appendix B. IT Governance Framework, describes the regulations, best practices and leading IT Governance schools of thought on which this document was based.

2 IT Governance Overview

The OI&T requires effective IT Governance to align IT strategy, systems, and processes to business strategy to realize cost savings, efficiencies, and improvements. IT Governance is responsible for determining how IT processes are established and enforced, and how and by whom IT decisions are made.

2.1 The Need for IT Governance

The effective management of information, information systems and communications is of critical importance to the success and survival of the VA. This criticality arises from:

- The pervasiveness of and dependence on information and the services and infrastructure that deliver the information
- The increasing scale and cost of current and future technology-related investments
- The potential for technologies to enable the transformation of the VA and its business practices
- Significant risk in technical and business initiatives
- Significant challenges in change management within the VA
- The speed and ease that large amounts of sensitive information can be transmitted

In addition, there is an increasing demand for generally accepted guidelines for decision making and benefits realization related to VA IT-enabled business investments. The management practices that traditionally have been applied are no longer sufficient. There is a clear incentive for management to ensure that effective IT Governance and management processes are in place to create value through optimizing benefits at an affordable cost with an acceptable level of risk.

For IT Governance to be successful at the VA, it should be a workable solution able to deal with the challenges and pitfalls presented by IT. It should not only prevent problems but also enable better services to our employees, veterans and their dependents; Administrations; and Staff Offices. IT risks are closely related to business risks, because IT is the enabler for most business strategies. The management and control of IT should, therefore, be a shared responsibility between the business and the IT functions with the full support and direction of the board. IT Governance provides the oversight and monitoring of activities within the broader VA-wide governance framework.

As the successful use of IT becomes more critical to the VA's success, the cost of doing nothing will far outweigh the cost of implementing IT Governance, which can reduce losses in other areas. For example, losses can include with security incidents, failed projects, and operational outages. Implementing enhanced IT Governance mitigates these risks and leads to realizing the effectiveness and efficiency benefits created by IT-enabled operational improvements.

Top management concerns need to be resolved by effective and timely measures promoted by the governance layer of the VA.

2.2 IT Governance Focus Areas

IT Governance best practices describe five focus areas for IT Governance: strategic alignment, value delivery, risk management, resource management and performance management. Managing all five areas is required for effective IT Governance. Strategic alignment is the alignment of IT strategy with business

strategy. Value delivery is realizing the business benefits intended through properly developing, operating and maintaining IT. Risk management is the process of monitoring, managing and mitigating IT risks. Resource management entails establishing and deploying the right IT capabilities for business needs at the right cost. Performance management is the monitoring and correcting of IT processes, which is fundamental to the success of all the IT Governance management processes.

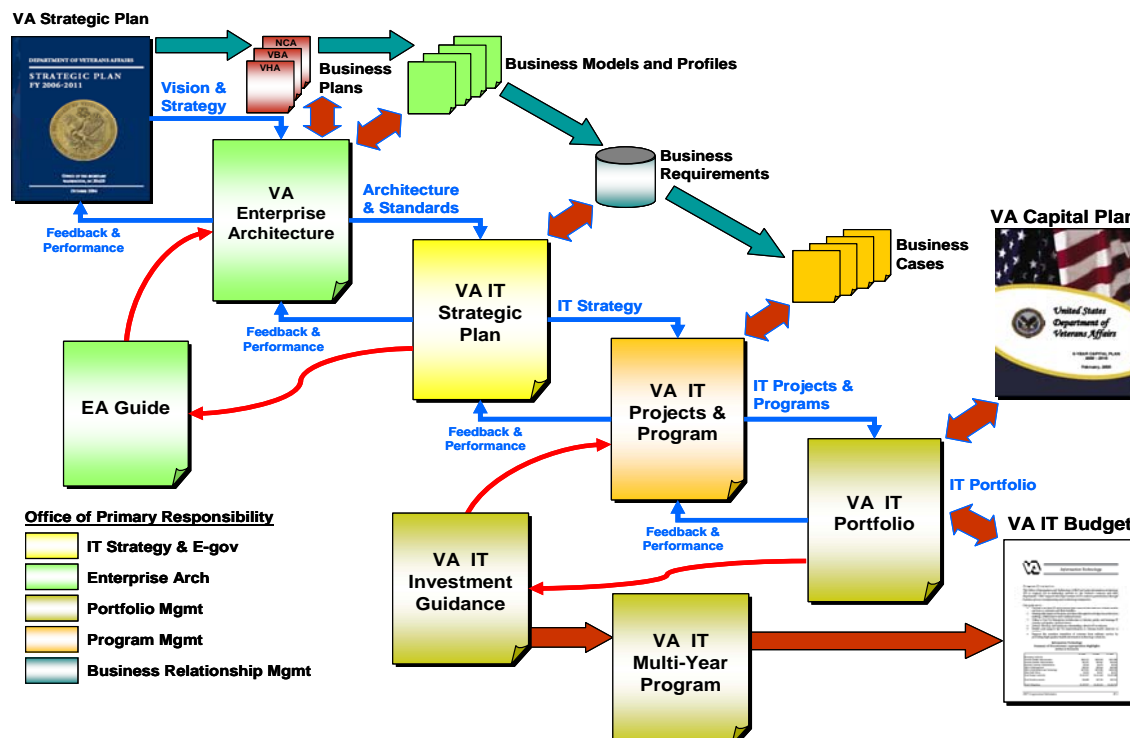
2.2.1 Strategic Alignment

A clear understanding of the internal and external business environment provides the required input for setting the IT function's mission, vision and strategy, while ensuring that the IT function's services are aligned to all elements of the department's environment. This is important to ensure that common values and strategic direction are shared and subscribed to throughout the VA.

Strategic alignment is needed to:

- Ensure that IT strategy is *aligned* with business strategy and that distributed IT strategies are consistent and integrated
- Ensure that IT *delivers* against the strategy (delivering on time and within budget, with appropriate functionality and the intended benefits – a fundamental building block of alignment and value delivery) through clear expectations and measurement
- *Balance investments* between systems that support the enterprise, transform the enterprise and create an infrastructure that enables the businesses to grow in new arenas
- Make decisions about the *focus* of IT resources, that is, their use to improve customer satisfaction
- Assure coordination of changes in VA policies, organization, staff training, equipment, leadership education and incentives, personnel, and facilities required for full realization of the expected benefits of investing in IT solutions

The Illustration below defines the strategy relationship emanating from the Secretary through the business units and to the enterprise architecture resulting in VA IT investment and budget priorities. *It codifies strategic goals, objectives, performance target and business needs with IT projects, programs and budget.* It reflects key IT processes and adds rigor to planning and enable measurement of investments.



Achieving a strong linkage to the business goals is essential for IT to ensure that it supports all parts of VA, its employees, veterans and their dependents by delivering services on time, with appropriate functionality and by achieving the intended benefits.

2.2.2 Value Delivery (Value Creation)

To achieve new levels of effectiveness and efficiency in executing its mission, the VA must implement new processes, practices, and procedures in key areas of its operations. This is the endpoint of creating value. The role of new products and services in handling information can create value only through the enablement of new business processes, practices, and procedures. To this end, complete alignment and coordination of funding and schedule for new initiatives is necessary in all aspects of VA policy, organizational change, staff training, equipment, leadership education and incentives, personnel management, and facilities.

The basic principles of IT value are delivery on time, within budget and with the benefits that were intended. IT processes should be designed, deployed and operated in an efficient and effective way that meets delivery expectations and objectives. These expectations and objectives are determined by the business value drivers, which are also influenced by environmental factors.

The value that IT delivers should be aligned directly with the values on which the business is focused, and be measured in a way that transparently shows the impact and contribution of the IT investments in the value creation process of the VA.

The level of efficiency and effectiveness of the IT processes depends on their maturity level, i.e., their level of capability and, if necessary, how they need to be improved to an appropriate or desired level.

Successful delivery of IT value for the VA requires a partnership between the business and the OI&T, and shared responsibility and decision making by business and IT management on sourcing decisions.

2.2.3 Risk Management (Value Assurance)

Whereas value delivery focuses on the creation of value, risk management covers the value assurance processes. Internal control requirements and the need to demonstrate sound VA-wide governance to veterans, service members, employees, other beneficiaries, and stakeholders are the main drivers for increased risk management activities in the Department. In addition to traditional financial risk management, regulators are increasingly concerned about information protection, data security, and operational and systemic risks. As a result, integrated risk management becomes more important to create transparency and improve accountability.

Risk management should be a continuous process that starts with the identification of risks (impact on assets, threats and vulnerabilities). Once identified, risks must be mitigated by countermeasures (control). But attention still needs to be paid to, and acceptance formally made of, residual risk. The performance of the risk mitigation process (including risk acceptance) should be managed, i.e., measured and monitored. Activities that the VA must manage, measure, and control include:

- *Security of its systems and the privacy of its employees', our veterans' and their dependents' data going forward – this is mandated by the Federal Information Security Management Act (FISMA) and it is a collective responsibility of all VA Administrations, Staff Offices, and staff alike;*
- *Unauthorized disclosure of Personally Identifiable Information (PII);*
- *Information-related financial resources, to assure that the VA receives full value for funds expended;*

- *Information-related human resources to assure that the workforce has the skills required to perform their evolving duties;*
- *Information and technology-related products and services to assure progress in accordance with plan.*

2.2.4 Resource Management

Resource management is about establishing and deploying the right IT capabilities for business needs at the right cost. It primarily targets human resources, including knowledge, skills, and abilities. Resource management deals with strategic sourcing of processes, considering both in-house and outsourcing models, and using evaluation criteria derived from the VA's strategic intent and critical success factors. It enables the VA to leverage knowledge and skills internally and externally. It promotes IT resource allocation transparency and adjudicates IT resource issues impacting on business needs.

Resource management ensures that an economical suite of information and technology management capabilities are provided to achieve the mission and the goals of the VA. Information and technology products and services are not ends in their own right. Investment in information and technology tools and techniques must be focused on optimizing service to our employees, veterans and their dependents; and stewardship of internal VA resources.

Only within this context is new technology introduced, as required by the business; trusted providers are used, and obsolete systems are updated or replaced. Resource management recognizes the importance of people, in addition to hardware and software, and, therefore, focuses on maintaining resource availability, providing training and skills development, promoting retention, and ensuring competence of key IT personnel.

IT assets should be organized optimally to provide the quality of service required to support the business objectives of VA, in the most cost-effective manner that is practical. Enterprises that achieve this not only realize great cost savings but also are well placed to take on the next new IT initiative, judiciously introducing new technologies and replacing or updating obsolete ones as required by emerging business needs.

To be successful, VA must align and prioritize the existing Information and Technology services that are required to support business operations based on clear service definitions. These definitions and related performance metrics enable business-oriented service level agreements providing a basis for effective oversight and monitoring of both internal and outsourced IT services.

2.2.5 Performance Measurement

Without establishing and monitoring performance, it is unlikely that the previous focus areas (strategic alignment, value delivery, risk management and resource management) will achieve their desired outcomes. Performance measurement includes audit and assessment activities on a continuous basis, and provides a link back to the strategic alignment phase by providing evidence that the direction is being followed. This also creates the opportunity to take timely corrective action, if needed.

Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency, and the ability to learn and grow.

Each perspective is designed to answer one question about the VA's way of serving its employees, our veterans, and their dependents:

- Veteran perspective – To achieve our financial objectives, what veteran needs must we serve?

- Financial perspective – To satisfy our veterans, service members, employees, other beneficiaries, and stakeholders, what financial objectives must we accomplish?
- Learning perspective – To achieve our goals, how must the VA learn and innovate?
- Internal process perspective – To satisfy our veterans, service members, employees, other beneficiaries, and stakeholders, in which internal business processes must we excel?

By using the balanced scorecard, managers rely on more than short-term financial measures as indicators of the company's performance. Managers also take into account such objectives as the level of veteran satisfaction, streamlining of internal functions, creating operational efficiencies, and developing staff skills. This view of business operations contributes to linking strategic objectives with tactical actions.

IT not only contributes information to the business scorecards and tools to the different dimensions being measured, but also – because of the criticality of IT itself – needs its own scorecard.

All IT Governance layers within the VA must make a high priority: (1) defining IT goals that align to VA businesses which are clear and explicit, and (2) measuring the level of their achievement. The achievement of IT goals must be continuously measured to determine the value IT is adding to VA business goals.

2.2.6 Linking the Five Focus Areas of IT Governance to the VA

For the OI&T to operate effectively, all five focus areas of IT Governance must be addressed (see Figure 1). “Strategic Alignment” aligns the IT strategy to the VA-wide business strategy and assessing the VA-wide IT needs, so that the best strategies can be realized. “Value Delivery (Value Creation)” implies that the VA needs to raise the Capability Maturity Model (CMM) rating across all of the Department so that IT is part of an integrated Department-wide capability to enable new processes in the Administrations and Staff Offices to provide better healthcare, benefits, and other services to its customers – the veterans, service members, employees, other beneficiaries, and stakeholders. “Risk Management (Value Preservation)” requires focus on reducing the IT risks to the VA to protect veterans’ information and the VA infrastructure. “Resource Management” guides the VA when providing quality human and non-human resources, which increases the effectiveness of employee hiring and retention, and procurement right sourcing. “Performance Measurement” enhances the VA’s ability to measure and manage its budget, serve the veterans’ needs, train its employees, and generally operate effectively and efficiently.

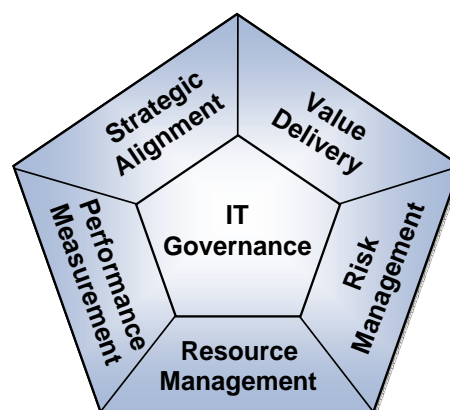


Figure 1 - IT Governance Focus Areas

Foremost among these five focus areas is effective performance measurement, so that corrective actions can be applied at the right time to the right IT Governance area.

2.3 VA-Wide Governance and VA IT Governance

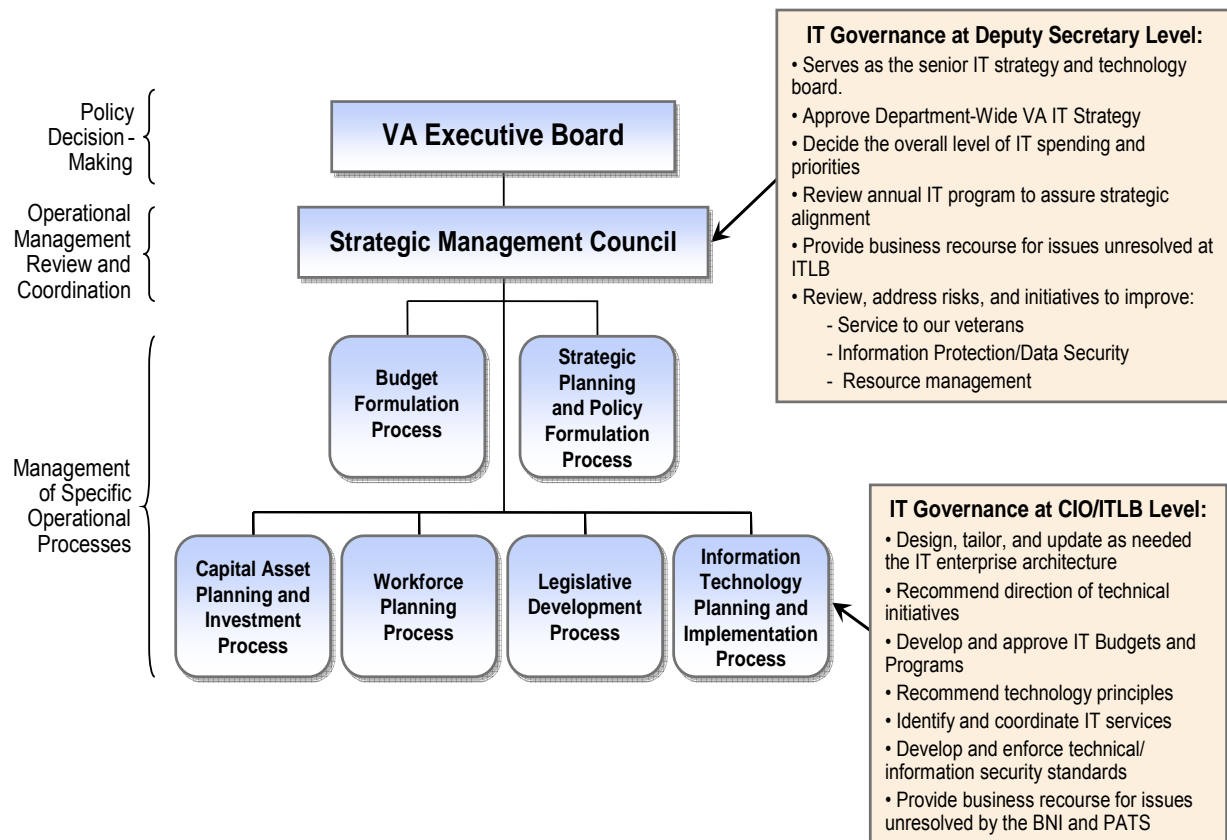


Figure 2 - Where IT Governance Fits into Governance at the VA

One of the principal goals is to align IT strategy to the VA business strategy. Figure 2 depicts where the IT Planning and Implementation process fits into the VA-wide governance decisions, which support aligning the OI&T to the VA-wide business goals.

2.3.1 VA-Wide Governance

VA-wide, or Department-wide governance, for the VA is governance in a broader sense than just IT Governance and is commonly referred to as enterprise governance. Department-wide governance is made up of the set of responsibilities and practices exercised by the VA Executive Board and executive management with the goals of providing strategic direction, ensuring that objectives are achieved, ascertaining that all risks (information protection/data security, financial, developmental and operational) are managed appropriately, and verifying that the VA's resources are used responsibly. Governance developments have primarily been driven by the need for transparency of department-wide risks and to ensure veterans, service members, employees, other beneficiaries, and stakeholders and their families are receiving the benefits they deserve. Because technology is the principal vehicle for the sending, receiving, processing, storing, and securing of information, there is a critical dependency on IT that calls for a specific focus on IT Governance.

2.3.2 VA IT Governance

IT Governance is the responsibility of the VA Executive Board, Strategic Management Council, and other executive managers, and not just the responsibility of the OI&T. It is an integral part of Department-wide governance and consists of the leadership and organizational structures and processes that ensure that the department-wide IT sustains and extends the VA's strategies and objectives.

IT Governance can be seen as a structure of relationships and processes to direct and control the VA to achieve its Department-wide goals by adding value, while balancing risk versus return over IT and its processes. IT Governance provides the structure that links IT processes, IT resources, and information to VA-wide strategies and objectives. IT Governance provides for coordination of changes in VA policies, organization, staff training, equipment, leadership education and incentives, personnel, and facilities required for full realization of the expected benefits of investing in IT solutions.

Furthermore, IT Governance integrates and institutionalizes best practices of planning and organizing, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance to ensure that the Department's information is available and secure and related technology supports its business objectives. IT Governance enables the VA to take full advantage of its information, thereby maximizing benefits to our employees, veterans, and their dependents by capitalizing on opportunities for better service. IT Governance also identifies control weaknesses and assures the efficient and effective implementation of measurable improvements.

3 VA IT Governance Model

A redesign of the VA's current OI&T and IT Governance structure is required. The IT organization and the business lines will have to change the manner in which they operate, and VA senior management will need to play an active role in IT Governance. It is very important to introduce some of the preliminary concepts that will be further refined as progress is made. The VA IT Governance Model is a high-level description of IT Governance Decisions, how VA IT Governance Boards are to be configured, which boards make what decisions, and the VA IT Governance Approach to beginning the redesign of IT Governance within VA.

3.1 IT Governance Guiding Principles

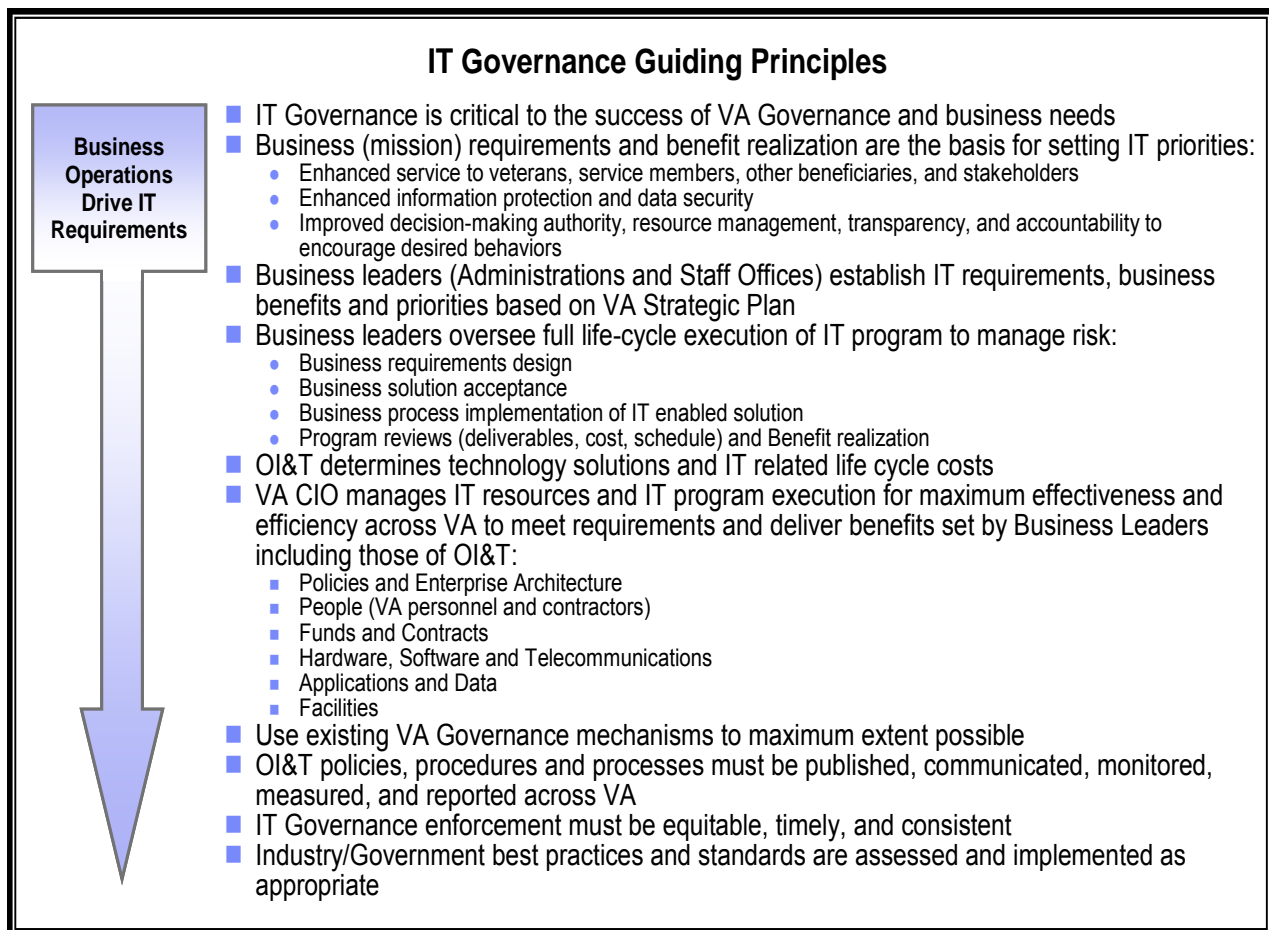


Figure 3 - IT Governance Guiding Principles for the VA

The establishment of IT Governance Guiding Principles is crucial to the successful implementation of IT Governance at VA. These principles must specify the input rights, decision making authority and accountability to encourage desirable behaviors in the use of IT. Managers must be made responsible for the policies, procedures, and processes required for their functional areas; and these policies, procedures and processes must be officially published and communicated so that they can be enforced. Compliance with these policies, procedures, and processes must be continuously monitored, measured, and reported. In addition, management action and enforcement must be equitable, timely, and consistent. Finally, industry best practices and standards should be assessed to determine their value in improving IT Governance at VA. These principles have been tailored for the VA and are described in Figure 3.

3.2 IT Governance Decisions

There are three types of IT Governance decisions that must be made:

- **Enterprise Architecture.** In accordance with the OMB-sponsored Federal Enterprise Architecture (FEA) Framework and the GAO Enterprise Architecture Maturity management Framework, the top-level leaders of the VA must in unison adopt an approach for creation, use, and maturation of all levels of the FEA for the purposes of: (1) adapting IT to the VA strategic plan, (2) ensuring alignment of IT initiatives to business vision for service and goals, (3) supporting business processes, information and technology solution development, (4) managing IT infrastructure, and (5) adhering to agreed-upon standards relevant to the mission of the VA.
- **IT Stakeholder Requirements.** Determine the functional requirements for both the Administrations and Staff Offices for applications, hardware, network infrastructure, and information protection. (ITGI “IT Governance Implementation Guide, Using COBIT and Val IT”, 2nd Edition”, Rolling Meadows, IL, 2006). Enterprise Architecture provides a blueprint for stakeholder requirements.
- **IT Investments.** Assure alignment of IT investments to VA Strategic Plan. Recommend the programming and budgeting of resources against the IT business plan, and its ability to meet customer demand, the priorities, and the funding allocation according to the Administrations and Staff Offices needs and requirements. (OMB Circular A-11, Section 300 Planning, Programming, Budgeting, Acquisition, Planning, Budgeting, Acquisition, and Management of Resources, 2006). A robust enterprise architecture provides the framework and foundation for IT capital investment planning.

Direction setting, decision making, and oversight boards must address these three areas to assure Departmental objectives are achieved. Specifically, the Administrations and Staff Offices will have decision rights for their business requirements (as discussed above), and will be expected to have open and direct communications with OI&T on a continuous basis during the full lifecycle of product development or procurement. The VA CIO will have decision rights with respect to IT strategy, services, technology and information assurance requirements. While other *decision rights* will be reserved for the VA CIO, Deputy Secretary and Secretary, leaders from Administrations and Staff Offices will have *input rights* on all applicable boards/committees to ensure full consideration of their business requirements and the operational effectiveness and suitability of IT solutions prior to implementation across the Department. For those functional requirements that relate to the business processes of the Administrations and Staff Offices, quality checkpoints will exist for user-driven design, user acceptance testing in accordance with approved test plans, and determination of the effectiveness and suitability of IT products with respect to evolving business needs.

Furthermore, the Administrations and Staff Offices will have recourse by making their business cases to the VA CIO, the Strategic Management Council (SMC)/ Deputy Secretary, and, lastly, the VA Secretary as the ultimate decision maker where warranted. Most importantly, VA's IT Governance implementation must remain focused on ensuring that the VA provides world-class IT services and support to the Administrations and Staff Offices in meeting strategic requirements to serve veterans, service members, employees, other beneficiaries, stakeholders and their families, and manage the resources of the VA.

3.3 VA IT Governance Boards

IT Governance is not an isolated discipline. It should form an integral part of VA Governance and needs to be addressed at the most senior levels of leadership. Senior leaders must ensure that IT operational risks are mitigated, and the value that is returned by technology investments meet the strategic goals and objectives of the VA. One of the most effective mechanisms for helping to establish governance over IT is an IT strategy and technology board. This board will be comprised of people at the most senior levels for setting or approving OI&T direction and providing high-level oversight. The SMC will serve as the IT strategy and technology board, which will directly link to the current VA Governance Framework. Below the SMC will be a number of Department level boards focusing on specific areas of the business and technology, such as prioritization of IT investments in business solutions, IT policies and standards, etc.

It should be recognized that day-to-day communication between the Administrations and Staff Offices with various OI&T offices will continue and is encouraged in order to ensure close coordination between the businesses and OI&T.

Development projects will follow normal project life cycles, such as a "Systems Development Life Cycle (SDLC)", where milestones are established and the OI&T development personnel and the customers (Administrations, Staff Offices or OI&T itself when it is the customer) will review the project for meeting requirements, being on track and within budget. This interaction between OI&T and its customers will constitute a form of quality check points to assure requirements and expectations are met between OI&T and its customers. This interaction and collaboration will begin with business concept creation through requirements definition, design, development, testing, customer acceptance, and deployment (See Figure 4 for an illustrative example of an SDLC). After deployment, the interaction will continue to assure the application/service meets the agreed business requirements, and it is modified as the business needs change until there is no longer a need for that particular application/service, and it is retired. This is the normal day-to-day work of a typical well managed IT organization.

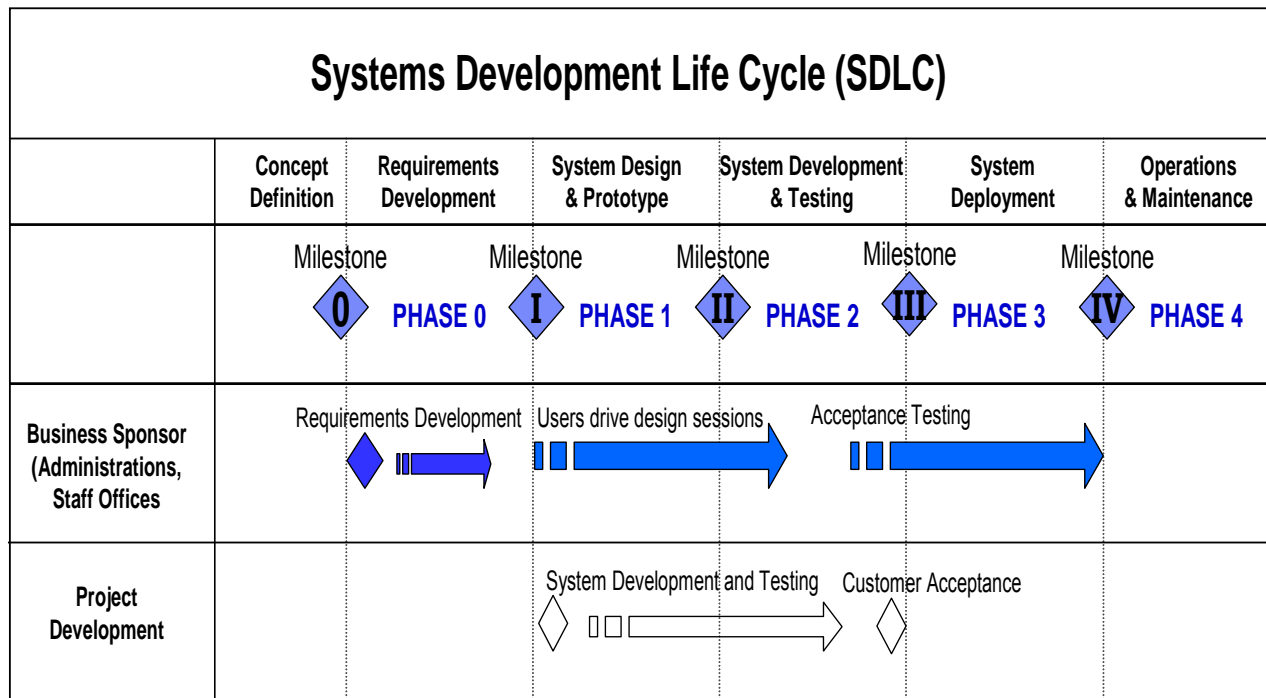


Figure 4 - Systems Development Life Cycle (SDLC)

Differences should first attempt to be resolved at the day-to-day working levels, then, if needed, be escalated to the appropriate management levels. Only when necessary should larger issues be escalated to the IT Governance board levels. It is not envisioned that IT Governance boards will be involved in the day-to-day functions of the business areas or OI&T, but they will provide departmental IT direction, oversight, prioritization, enforcement, and issue resolution.

Based upon IT Governance best practices, it is recommended that VA establish three Department-level strategy IT Governance boards—the *IT Leadership Board (ITLB)*, the *Business Needs and Investment (BNI) Board*, and the *Planning, Architecture, Technology and Services (PATs) Board*, and use the existing VA Governance model to the maximum extent possible. For example, the *SMC* exists today; so there is not a need to recreate a similar or duplicate board. The relationship among these boards is pictured in Figure 5.

In addition to the IT Governance Boards, a *Business Advisory Committee* will be established. This *Business Advisory Committee* will be primarily focused on advising the *ITLB* on user acceptance testing and training within the scope of IT projects and will collect objective data as a basis of feedback to the *ITLB*.

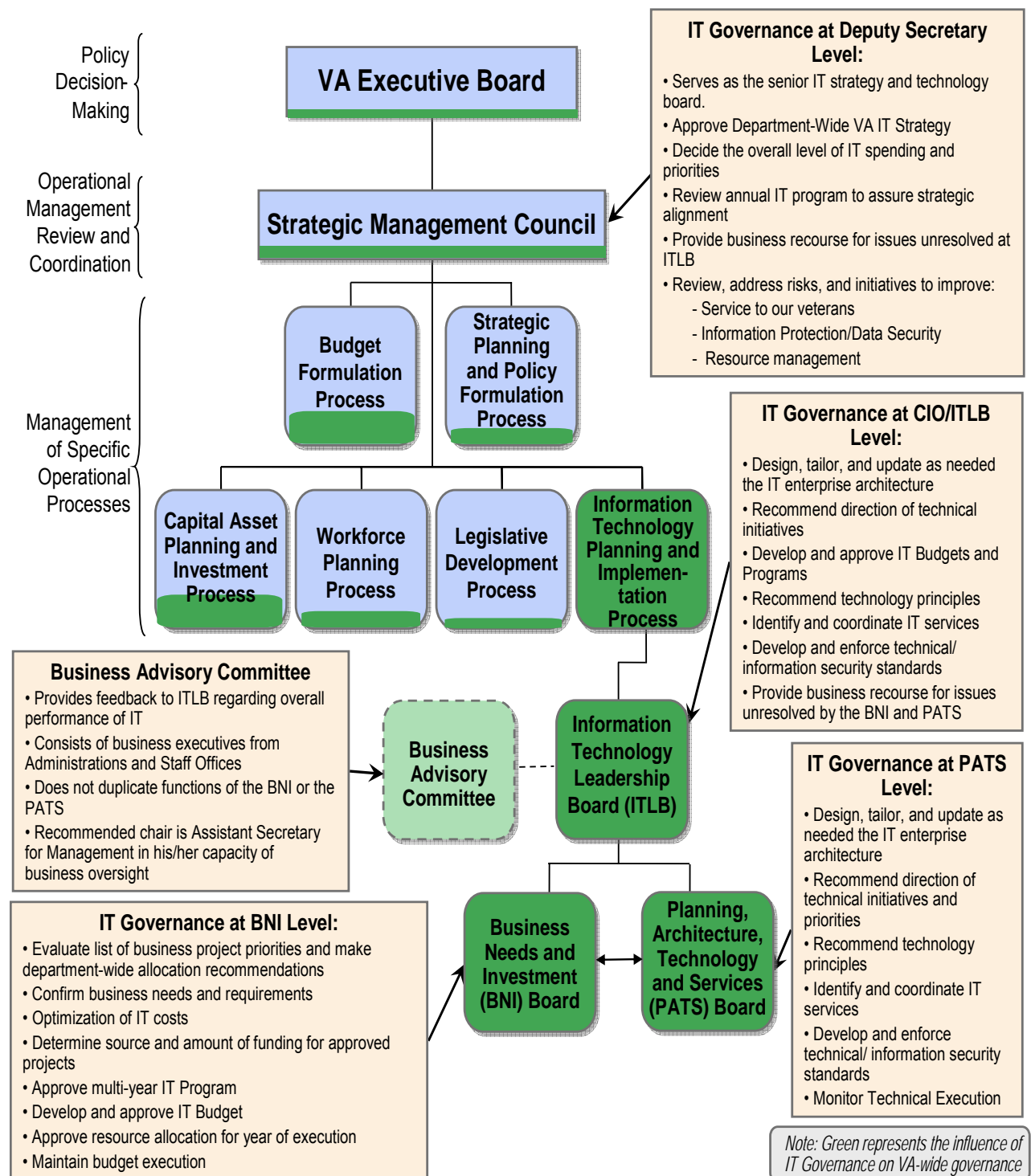


Figure 5 - VA IT Governance Board Structure

	SMC	IT Leadership Board (ITLB)	Business Needs and Investment (BNI) Board	Planning, Architecture, Technology and Services (PATS) Board
Level	Department-Wide Enterprise Strategy	Department-Wide Enterprise Strategy	Department-Wide Enterprise Strategy	Department-Wide Enterprise Strategy
Purpose	VA priorities, align IT to business, Risk Management, IT Governance	IT Strategy, Align IT strategy to business, IT Performance	Business Needs Satisfaction, Investment Control	Develop Enterprise Architecture, IT Principles and Standards, Technology Enhancements
Responsibility	<ul style="list-style-type: none"> Decides the overall level of IT spending Aligns and approves enterprise IT architecture Approves project plans and budgets, setting priorities and milestones Determines alignment to business requirements and resolves conflicts between IT projects competing for funding Accepts IT Risks Assures enforcement and reporting of IT Governance Provide business recourse for issues unresolved at ITLB 	<ul style="list-style-type: none"> The alignment of IT with the business Determine achievement of IT objectives Determines availability of IT resources and takes appropriate actions Develop and approve IT Budget and Programs Manages progress on major IT projects Performance Management of IT Services Management of IT Strategic Plan Develop and enforce information protection/data security policies and processes. Develop and enforce IT Policies Exposure and containment of IT risks Design, tailor and update the information architecture as needed Provide business recourse for issues unresolved by the BNI and PATS Assess and approve IT Budget 	<ul style="list-style-type: none"> Confirm business needs and requirements Review funding requests Optimization of IT costs, including value delivery Oversees risk, and return of IT investments Determine source and amount of funding for approved projects Monitor project achievement of results Oversee multi-year programming Formulate and approve IT Budgets and Programs Monitor IT budget execution Determine Budget performance metrics 	<ul style="list-style-type: none"> Design, tailor, and update as needed the IT enterprise architecture Recommend direction of technical initiatives Recommend resolutions to architecture and technological issues Recommend technology principles Develop and enforce technical standards Plan and collaborate technology upgrades Oversight of Engineering Changes Recommend new IT Services Maintain IT services catalog Develop and maintain information security architecture Review and analyze deployed information technology Evaluate list of business project priorities and make Department-wide recommendations Monitor IT execution
Authority	The senior IT Governing body, sets policies, and resolves disputes of IT boards.	Approve IT direction, manages IT Strategic Plan and oversees IT Governance & Information Security, IT Performance., and IT Resources.	Receives business case and funding requests, recommends funding, monitors progress and value of projects.	Designs IT Architecture, recommends IT principles, IT strategic plan, standards & solutions, collaborates technology enhancements, and coordinates IT Services.
Membership	Most senior officers in the VA, the Deputy Secretary, COOs of VA Administrations and department CXXs. The Deputy Secretary is the Chairperson.	ASIT, ASIT direct reports, executives representing the administration and staff offices, and the IT Governance executive. The Assistant Secretary for Information and Technology (AS/IT) CIO is the Chairperson.	Senior executives representing the Administration and Staff Offices, the resource management officer(s), the IT Service Managers providing direct support to the business areas, Enterprise Architect, and the IT Governance executive. The Principle Deputy Assistant Secretary of OI&T is the Chairperson.	IT service managers, Chief engineer, Senior executives representing the Administration and Staff Offices, business executives with expertise in understanding business impacts of IT, Enterprise Architect, and the IT Governance executive. The Deputy Assistant Secretary for Information and Technology (AS/IT) Enterprise Strategy, Policy, Plans and Programs is the Chairperson.

Table 1 - VA IT Governance Boards

In Table 1, the relationships among these boards are summarized. It provides each board's name, level, and purpose; and summarizes each board's responsibility, authority, and membership. Based upon further implementation of IT Governance within VA, additional boards and committees can be created based on the operations-level, domain-level, and process-level needs.

These VA IT Governance Boards will provide Department-wide implementation planning, based on the foundation of the developed IT processes. Each of the IT processes adopted by the VA for implementation will require the IT community to apply these process principles in IT Governance to optimize the decision making capabilities for each board. Inclusion and participation of business executives will be a critical for the IT Governance structure to become operational.

It should also be noted that the Enterprise Architect should be a member of both the *BNI* and *PATS*, since the Enterprise Architecture will address both the business information and technology architectures, and should influence both long-term and short-term business transformation and the IT projects that support that transformation. The Enterprise Architecture ultimately will identify the "blue print" that represents the way forward.

3.3.1 Strategic Management Council (SMC)

The current *SMC* serves as the senior board making decisions related to IT strategy and technology. It is chaired by the Deputy Secretary. This board may also use IT experts to serve as technical advisors should the need arise. The IT Governance Framework accommodates the *SMC* in this role. The *SMC* provides business recourse for issues unresolved at *ITLB*. The board will meet at least quarterly and probably much more frequently during the early stages of IT Governance implementation. The objective of this board is to assure the alignment of IT and business requirements, delivery of value by IT to the Administrations and Staff Offices, measurement of IT performance, management of IT/Information Security related risks, and oversight of sourcing and use of IT resources. *This board is the strategic, priority setting, oversight and issue resolution board for IT matters within VA.*

3.3.2 IT Leadership Board (ITLB)

The *IT Leadership Board (ITLB)* will be the first Department-wide IT Governance board; it will address all information resources management areas: strategy, programs, projects, services, and issues as they arise. It will be chaired by the Assistant Secretary for Information and Technology (AS/IT); members will include key Executive leaders in OI&T, Administrations, and Staff Offices. This board will meet at least monthly but may meet more often if needed. The objective of this board is to set Department-wide information, security, and technology direction, based upon business requirements and technology evolution; ensure the VA IT Strategic Plan supports the goals and objectives of the VA Strategic Plan; approve and enforce IT policies; protect information and data, recommend and manage IT infrastructure investments; and monitor the performance of the IT services. The *ITLB* will provide business recourse for issues unresolved by the *BNI* and *PATS*. *This board will represent the information and technology services, strategies, principles, governance, and resources for all IT that support business organizations across VA.*

3.3.3 Business Needs and Investment (BNI) Board

The *Business Needs and Investment (BNI) Board* will be a Department-wide IT Governance board that address IT services and solution development activity realization of business solutions. It will be chaired by the Principle Deputy Assistant Secretary (PDAS) of OI&T. While the PDAS of OI&T will normally chair the *BNI*, any of the OI&T DAS may be designated the chairperson depending on the subject matter

being addressed. The BNI will comprise senior executives representing the Administrations and Staff Offices, resource management officers, and selected IT service managers. This board will meet at least monthly and possibly more frequently during program/project/budget development windows. The objective of this Committee is to identify, review, recommend, and advocate IT projects/programs across the Department (business solutions and new services for the business areas), monitor and realign IT business solution projects, and optimize IT resources. This board will oversee resources during full lifecycle of IT systems and oversees the total cost of ownership, which includes the cost to secure and protect information and data throughout the organization. This Board will enforce the use of enterprise architecture as the key planning tool and framework to document and analyze new functional requirements, thus assuring interoperability across VA, and identification of key overlaps and gaps in IT programs. This Board will make recommendations to the ITLB on IT related projects and programs that address business requirements and needs. This board will focus heavily on the resource aspects within the VA, multi-year programming and budget formulation, and budget execution, ensuring that are all developed and approved at the BNI board level. The chairperson will also convene comprehensive program reviews of key IT related projects and initiatives to assure continued alignment to business priorities and maximum value of investments. The BNI will adjudicate all IT resource issues; unresolved issues will be forwarded to the ITLB. *This board will represent the business units and their needs/requirements for investments in IT and will monitor the fulfillment of those needs.*

3.3.4 Planning, Architecture, Technology and Services (PATS) Board

The *Planning, Architecture, Technology and Services (PATS) Board* will be another Department-wide IT Governance committee. It will oversee the technical performance delivery of IT services, development of enterprise architecture – including the information security and IT infrastructure. It will be chaired by the Deputy Assistant Secretary for IT Enterprise Strategy, Policy, Plans, and Programs. It will comprise senior executives representing the business requirements of the Administrations and Staff Offices, Enterprise Architect, Systems Engineer, selected IT service managers, and business executives selected for their knowledge and expertise in understanding business impacts of IT. This board will meet at least monthly but may meet more often if needed. The objectives of this board are to (1) formulate and enforce VA Enterprise Architecture, (2) oversee the creation the VA IT Strategic Plan and the service level agreements that OI&T has in place with its customers for reliability, availability, security and maintainability of the IT infrastructure, and (3) meet performance (processing speed) requirements of those agreements. This board will evaluate the list of business project priorities and make Department-wide recommendations; oversee technology upgrades; approve new, more efficient infrastructure designs and services; and provide oversight of engineering change activities. By being the board that reviews and prioritizes all new IT related projects/programs across the entire VA, it will generally have both a moderate term (next 12-24 months) and long term (two to five years) view and will be tasked with the integrated priority setting of all to ensure maximum support to the VA's business plan and the most effective utilization of IT funds and resources. *This board will recommend the overall Departmental priorities for IT related business solutions and define IT Service offerings, infrastructure and technology architecture/standards; and it will be critical to assuring standardization, interoperability, security, reliability, and flexibility of the technology infrastructure.*

3.3.5 Business Advisory Committee

The *Business Advisory Committee* will be a non-governance body. It is established to provide business unit feedback to the ITLB regarding overall IT performance. This will include the operations and support of existing business requirements and needs. This group will be primarily focused on advising the ITLB on user acceptance testing and training within the scope of IT projects and will collect objective data as a basis of feedback to the ITLB. User acceptance testing and training will be developed in close

coordination with OI&T with the VA CIO, and approved by the ITLB in advance of execution. The *Business Advisory Committee* will provide an important feedback mechanism for the *ITLB* and will be comprised of business executives from the Administrations and Staff Offices. The *recommended* chair for this advisory committee is the Assistant Secretary of Management, in his business oversight role, to assure a Department-wide focus. This committee is a trusted advisory body to the ITLB; it is not intended to circumvent or duplicate the responsibilities and authorities of the IT Governance Boards (*BNI*, *PATS* or *ITLB*).

3.3.6 Other IT Governance Bodies

Based upon VA's IT Governance needs and the IT processes being implemented, additional boards/committees/groups probably will be formed to cover specific day-to-day activities, such as change management, architecture review, and project review, etc.

As the IT Process teams meet to identify and document their processes, the implications of IT Governance at the process level will be evaluated with the VA IT process owners. And, as a result, additional process-level IT Governance bodies may be created as deemed needed. However, when new IT Governance Boards are created, both the Administrations and Staff Offices will have representatives involved to ensure that business inputs and the resulting decisions are in accordance with business line and IT needs.

3.3.7 Example IT Governance Decision

To illustrate, at a high level, how the IT Governance boards should enable IT decision making, an example of IT Governance decision making is explained below.

In this example, the business need is identified and brought forward through the appropriate business line requirements prioritization process – before being presented to the *BNI*. The business need is reviewed and scoped, and life cycle costs will be estimated through the collaborative effort of the business representatives working with representatives of OI&T. This new need, in combination with all other needs in the business unit portfolio, will be presented to the *BNI* for review and consideration in comparison to the needs of the other Administrations and Staff Offices, within the constraints of available funding. The *BNI* will assess whether this new requirement requires a new project, can be incorporated into an existing initiative, or requires a combination of both. From the perspective of the Principle Deputy Assistant Secretary for IT, the *BNI* uses the Enterprise Architecture to assure that all interoperability requirements, process re-engineering initiatives, IT services and standards are addressed. The *BNI* assures Administrations and Staff Offices (including OI&T) requirements have been identified, documented, justified, scoped, planned, and prioritized and that funds are allocated for the Department. Next, the scoped, funded, and prioritized business needs are forwarded with all other prioritized requirements to the *ITLB* for review and endorsement and then on to the SMC for department-wide approval. For an example, see narrative below and Figure 6.

EXAMPLE:

1. The VHA may have a need for physicians in a cost-effective and efficient way to share thoughts and ideas on certain patients or problems with several colleagues at different locations across the country. These discussions should be supported by portions of patient records to assist in the diagnosis and treatment plan for the patient. There are more than 150 medical centers where this capability is needed, and the potential value of improving patient care is significant. The business unit scopes the project with OI&T counterparts, prepares justification and prioritization within the VHA, and submits input to *BNI*.
2. The *BNI* reviews the input to ensure scope, requirements, business case, size, and cost are adequately documented and enters the project input into a candidate project list. (The IT service managers on the

BNI will be critical in reviewing the scoping and cost estimating against existing services to validate the infrastructure component of lifecycle cost estimate, the likely recurring operations and maintenance cost of this project, and that the project follows the Enterprise Architecture blueprint.)

3. The new project or business requirement/technology will be forwarded to the *PATS* where it will be reviewed to see if it is a new IT Service, such as “web casts” in this case, to determine the most effective design/engineering approach in building, implementing, and operating this new technology, and an overall departmental priority will be established. Then *PATS* either recommends it be a new service where a new department-wide project is developed and scoped, which includes the requirements for the original business unit, or if the original project can be packaged with priority assignments and returned to the *BNI*.

4. The *BNI* then collects this project proposal and all project/service requests and allocates recommended funding of projects by priority and forwards recommended programs/projects/services with associated budgets to the *ITLB*.

5. Next, the *ITLB* reviews, modifies, or endorses the recommended priorities and funding. On at least an annual basis the VA Business and IT portfolios would go to the *SMC* from the *ITLB* with options and recommendations for approval.

6. The *SMC* would look at approving the portfolio as recommended, modifying it, or rejecting it and return findings to the *ITLB*.

7. The *ITLB* would accept the *SMC* decision and promulgate the implementation through the *BNI*.

8. The *BNI* then would assign the project to the appropriate business unit and OI&T to implement. The *BNI* would monitor the project from an investment value standpoint, and the project would be monitored by the business units for meeting business needs and OI&T for achieving the required service performance metrics.

9. The business unit would manage and execute the project.

Figure 6 presents a view of this process:

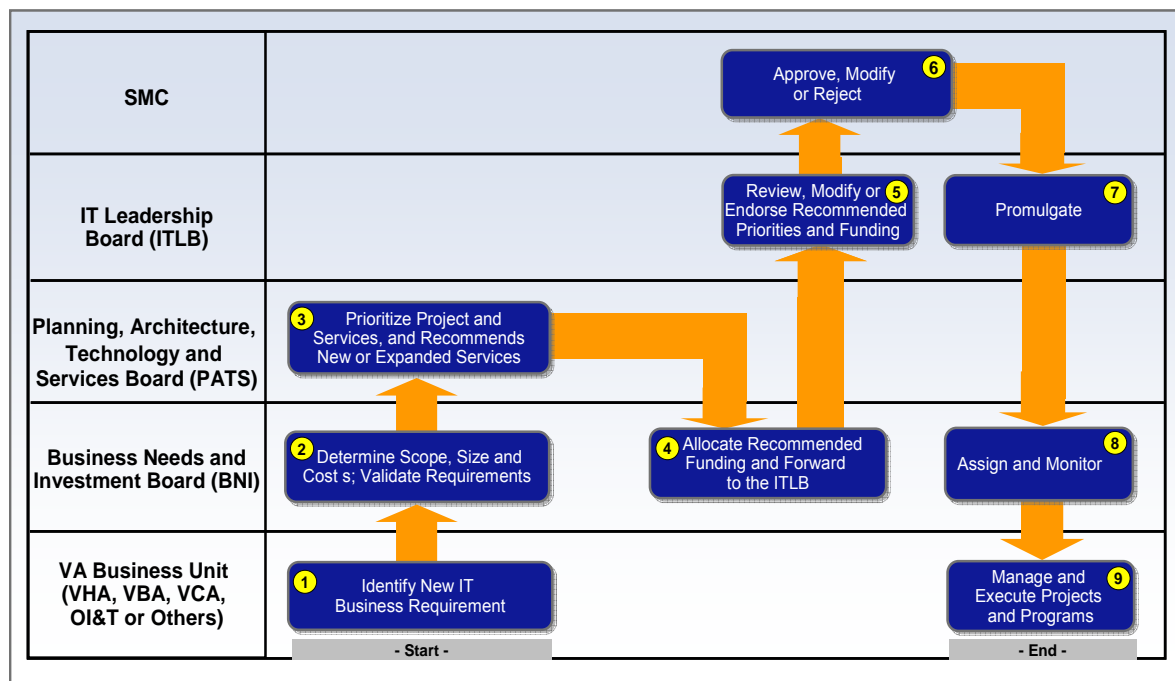


Figure 6 - Example IT Governance Decision Flow Chart

As the organization, processes and frameworks are more fully matured within VA, more detailed data capturing, input, process, and output specifics will be developed (and possibly more delegation from the SMC as well).

It should also be noted that the *Business Needs and Investment (BNI) Board* will be the key board for identifying and justifying the Administration and business unit needs and will be the body that allocates funding for projects/programs and makes recommendations via the *ITLB* to the *SMC* for departmental approval. The business will determine the needs and the priorities, the IT organization will determine technology solutions and will be held accountable to the business units for providing the IT solutions and the services they need to perform their missions – collectively providing exemplary service to veterans, service members, employees, other beneficiaries, and stakeholders.

3.3.8 Board Charters

The chairperson of each board, in collaboration with key board members, will need to take the information from Table 1, “VA IT Governance Boards” and build an expanded charter identifying specific scope, purpose, responsibilities and deliverables, authority, membership, terms of membership, frequency of meetings, documentation, processes, and support resources. These charters will need to be accomplished in the very near term after the IT Governance Plan has been accepted.

3.4 Road Map for Implementing IT Governance

The VA IT Governance Program is in the initial stage of needs identification when issues, challenges, and requirements will need to be defined and priorities established (see Figure 7).

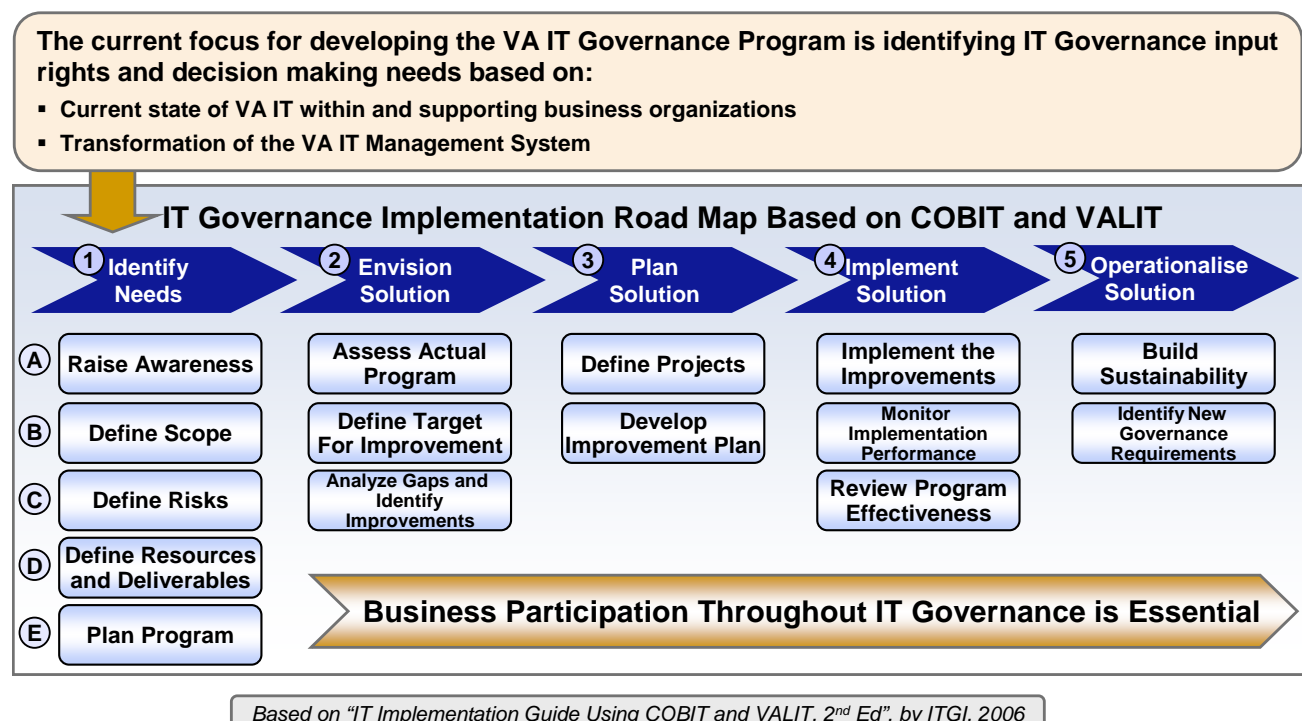


Figure 7 - Road Map for IT Governance Implementation

The outcome of the initial stage (Identifying Needs) of the road map for IT Governance Implementation will influence decisions on how fast, how far, and what resources will be used to implement IT Governance across the VA. In essence planning during the first stage delivers:

- Business Case
- Prioritized Goals and Objectives
- Risk Analysis
- IT Governance Framework within VA
- Program Organization
- Resource Plan
- Program Plan
- Communications Plan

Much of this initial work has already begun; is in various stages of completion; and needs to be quickly integrated and brought to closure to assure priorities projects/initiatives are properly resourced, planned and tracked. There is a considerable amount of change going on with the “VA IT community” and the business partners, Administrations and Staff offices. No organization can withstand all of this change at once. Careful consideration must be given to make sure the focus and resources are in the most critical areas and management attention given to assure quick success in those areas and plans to complete remaining are also communicated and tracked.

3.5 VA IT Governance Summary

The Administrations and Staff Offices will need to take their roles very seriously on the various IT Governance boards and assign well qualified and knowledgeable individuals to represent them on these boards – to ensure their inputs are understood and to influence the decision making to ensure approval for their critical business requirements. Furthermore, the boards must ensure transparency in their deliberations and decisions so that trust and respect are evident throughout the VA. IT Governance is intended to modify behavior to achieve better results and additional benefits VA-wide. Some of the improvements that will be achieved include:

- Standardized processes
- Alignment of business strategy to IT strategy
- Realization of business goals (e.g., responsiveness to veteran needs)
- Reduced security and privacy risks
- Optimized resource and asset utilization
- More cost effective use of IT
- More effective use of IT for:
 - Return on Investment (ROI)
 - Business flexibility
 - Improved service levels
 - Improved interoperability
- Measurement through the use of meaningful performance metrics

IT Governance implementation is a journey and not a destination. It will require significant VA senior management support and participation in building and enforcing the program, as well as more structure, discipline, and behavioral change within IT and the business areas. No longer will each organization be able to do as they wish without consideration of impact upon the entire VA, and customers including veterans, service members, employees, stakeholder and other stakeholders. In return customers will receive more dependable services by meeting the needs of the business and the assurance that the entire VA receives the full value for the IT investments.

The key is aligning the business and IT processes to ensure cost effective and efficient business solutions across all of VA in meeting the primary objective – exceptional services for our veterans, service members, employees, other beneficiaries, and stakeholders!

Appendix A. Reference

This section identifies reference materials.

Parent Documents

Parent documents establish the criteria and the technical need for the VA IT Governance Plan. The parent documents include the following:

- *IT Organization Directive 05-1, VA Administrations' Organization for IT Development, EDMS 337095*
- *Office of the Assistant Secretary for Information and Technology–Organization Book, High-Level Target Organizational Structure (December 2006)*
- *Task Delivery Order for Supplies or Services, Contract No. GS-23F-7107H, Order Number J67251*
- *Single Leadership Authority Structure of the VA Information Technology Management System (September 25, 2006)*
- *U.S. Department of Veterans Affairs: Federated IT Management System request for Quotation No: VA-101-06-RP-0031*
- *U.S. Department of Veterans Affairs: Federated Information Technology System Model (February 2006)*
- *U. S. Department of Veterans Affairs Information Technology Management Improvement Act of 2005*
- *Veterans Benefits, Health Care, and Information Technology Act (December 2006)*

Reference Documents

Reference documents serve as sources for best practices, industry standards, and government policy for the VA IT Governance Plan. The reference documents include the following:

- *House Report 109-256- Department of Veterans Affairs Information Technology Management Improvement Act of 2005*
- *IBM Process Reference Model for IT (PRM-IT) (2005)*
- *Information Technology Governance Institute (ITGI), "Board Briefing on IT Governance, 2nd ed.," Rolling Meadows, IL (2003)*
- *ITGI, "Control Objectives for Information and related Technology (COBIT) 4.0, Rolling Meadows, IL (2005)*
- *ITGI, "Enterprise Value: Governance of IT Investments, The Val IT Framework" Rolling Meadows, IL (2006)*
- *ITGI "IT Governance Implementation Guide, Using COBIT and Val IT", 2nd Edition", Rolling Meadows, IL (2006)*
- *Office of Management and Budget(OMB), Federal Enterprise Architecture Program EA Assessment Framework 2.0, (2005)*
- *OMB Circular A-11,Section 300 Planning, Budgeting, Budgeting, Acquisition, Planning, Budgeting, Acquisition, and Management of Resources (2006)*
- *United Kingdom Office of Government Commerce, ITIL: Information Technology Institute Library, Office (2006)*

Appendix B. IT Governance Framework

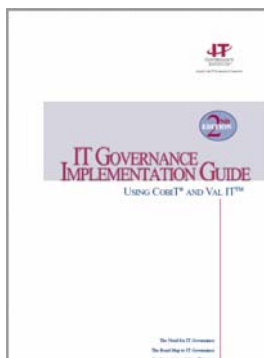
The IT Governance program will be based on government regulations and industry-wide best practices. Some of the key regulations and industry-wide best practices are:

Regulations

- Clinger-Cohen Act of 1996
- FISMA: Federal Information Security Management Act of 2002
- HIPAA: Health Insurance Portability and Accountability Act
- National Institute of Standards and Technology (NIST) Publications and Guidelines in support of FISMA
- Office of Management and Budget (OMB), Federal Enterprise Architecture Program EA Assessment Framework 2.0
- OMB Circular A-11, A-123, A-127, and A-130

Best Practices

- COBIT: Control Objectives for Information and related Technologies
- IT Governance Implementation Guide
- ITIL: Information Technology Institute Library
- PRM-IT: Process Reference Model for IT
- Val IT Framework



The process and framework to be followed is based on the IT Governance Implementation Guide 2nd Edition, published by the IT Governance Institute, 2006.

The IT Governance Institute is considered to have a comprehensive approach to IT Governance, which is often referred to as the “Gold Standard” for IT Governance. Other best practices will be incorporated as appropriate for specific service, process and support areas (see Figure 8).

The Proposed VA IT Governance Structure draws from all four schools, with a focus on ITGI.

	IT Infrastructure Library (ITIL)	The Process Reference Model-IT (PRM-IT)	Control Objectives for Information and related Technology (COBIT)	IT Governance Institute (ITGI) Board Briefing on IT Governance
Background	Developed by the UK's Office of Government Commerce in 1989, ITIL is a library documenting best practices for IT service, infrastructure, and application management.	The IBM Process Reference Model for IT (PRM-IT) is a generic representation of the processes involved across the complete IT Management domain.	Developed by the Information Systems Audit and Control Association (ISACA), COBIT defines IT activities in a generic process model within four domains: Plan and Organize; Acquire and Implement; Deliver and Support; and Monitor and Evaluate. Enables IT to be properly managed and controlled based on control objectives and management guidelines.	Developed by the ITGI to assist enterprise leaders in making IT successful in supporting the enterprise's mission and goals. It provides a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.
Scope	<ul style="list-style-type: none"> Align IT with the current and future needs of the business and its customers Improve the quality of IT service delivery Reduce the long-term cost of service provision 	<ul style="list-style-type: none"> Provides an integrated collection of IT processes Enable businesses functions Provide a basis for process assessment, design, and implementation 	<ul style="list-style-type: none"> Composed of a series of 34 IT processes with maturity models, critical success factors, key goal indicators and key performance indicators for each of COBIT's processes. Contains over 200 detailed control objectives supporting the 34 IT processes. 	<ul style="list-style-type: none"> Provides detailed guidance to ensure IT: <ul style="list-style-type: none"> - is aligned with the business - enables the business and maximizes benefits - resources are used responsibly - risks are managed appropriately Outlines varying levels of IT governance sophistication

Figure 8 - IT Governance Schools of Thought Drawn On